INFORMATION STORING APPARATUS

[0001] This patent application claims priority from a Japanese patent application No. 2003-005109 filed on January 10, 2003, and a Japanese patent application No. 2003-372722 filed on October 31, 2003, the contents of which are incorporated herein by reference.

BACKGROUND OF THE INVENTION

Field of the Invention

[0002] The present invention relates to an information storing apparatus storing thereon information. More particularly, the present invention relates to an information storing apparatus for setting access level for information for a person other than the owner of the apparatus.

Description of Related Art

[0003] A plurality of cards, such as an ATM card, a credit card, and a patient's registration card of a medical institution, are retained by a person. Research and development for integrating the cards into an IC card has been undertaken recently. (Cf. Seiichi Ido (ed.), "IC card information distribution platform, key technology of the 21st century information society", The Telecommunication Association, May 10, 2001).

[0004] The integrated IC card stores personal information. In this case, in order to provide protection of privacy of the IC card, it is necessary to set the access level for the personal information for the requester. Furthermore, it is necessary to prevent impersonation for acquiring the personal information.

SUMMARY OF THE INVENTION

[0005] Therefore, it is an object of the present invention to provide an information storing apparatus which can solve the foregoing problems. The above and other objects can be achieved by combinations described in the independent claims. The dependent claims define further advantageous and exemplary combinations of the present invention.

[0006] According to a first aspect of the present invention, there is provided an information storing apparatus storing thereon owner's personal information. The information storing apparatus includes: a personal information storing section storing thereon the personal information which is to be disclosed to predetermined accessible persons; an accessible person information storing section storing thereon accessible person characteristic information indicating a physical characteristic of each of the plurality of accessible persons; a requester authentication section for receiving requester characteristic information indicating a physical characteristic of a requester who requests the personal information, and for performing authentication processing of the requester using the requester characteristic information and the accessible person characteristic information stored on the accessible person information storing section; an access level setting section for setting an access level, which is a level of the personal information to be disclosed to the requester, when the requester authentication section authenticates the requester as the accessible person; and a personal information output section for outputting a part of the personal information stored on the personal information storing section to the

requester in accordance with the access level set-up by the access level setting section.

[0007] Moreover, the information storing apparatus may further include an access level storing section storing thereon a personal information level, which is a level of the personal information to be disclosed to the accessible person, in association with each of the plurality of the accessible persons, and the access level setting section may set the access level to the personal information level corresponding to the accessible person when the requester authentication section authenticates the requester as the accessible person.

[0008] Moreover, the information storing apparatus may further include an access level storing section storing thereon a personal information level, which is a level of the personal information to be disclosed to the accessible person, and an authentication criterion, which is strictness of the authentication to be performed when the personal information within the personal information level is disclosed, in association with each other, and the access level setting section may determine the personal information level corresponding to the authentication criterion as at least a part of the access level when the requester authentication section authenticates the requester by the authentication criterion or a criterion stricter than the authentication criterion.

[0009] Moreover, the requester authentication section may receive the authentication criterion from the access level storing section, the authentication criterion corresponding to the personal information level for the personal information requested from the requester, and the requester authentication section may perform authentication processing of the requester by the authentication criterion.

[0010] Moreover, the access level storing section may store the plurality of personal information levels and also stores a lower limit of credibility of the authentication as the authentication criterion corresponding to each of the personal information levels. The requester authentication section may output the credibility of the authentication for the requester based on the result of the comparison of the requester characteristic information with the accessible person characteristic information. The access level setting section may select the personal information level of which the lower limit of the corresponding credibility is less than the credibility of the authentication output by the requester authentication section, and sets the access level to the sum of the selected personal information levels.

[0011] Moreover, the access level storing section may store the personal information level and the authentication criterion in association with a title of the requester. The requester authentication section may further receive the title of the requester from a belonging of the requester, and performs authentication processing of the requester using the authentication criterion by reading the authentication criterion corresponding to the received title from the access level storing section. The access level setting section may set the access level to the personal information level corresponding to the title of the requester when the requester authentication section authenticates the requester as the accessible person.

[0012] Moreover, the accessible person information storing section may store a plurality of accessible person characteristic information of each of the accessible persons, and the requester authentication section may receive a plurality of requester

characteristic information, and performs authentication processing of the requester using the plurality of accessible person characteristic information and the plurality of requester characteristic information.

[0013] Moreover, the information storing apparatus may be retained by the owner.

[0014] Moreover, the requester authentication section may employ face information as the requester characteristic information and the accessible person characteristic information. Moreover, the information storing apparatus may further include an image capturing section for generating the requester characteristic information by capturing an image of the requester. Moreover, the requester authentication section may receive the requester characteristic information from a portable apparatus retained by the requester, and the personal information output section may output the personal information to the portable apparatus retained by the requester and causes the portable apparatus to store the personal information.

[0015] According to a second aspect of the present invention, there is provided an information storing apparatus storing thereon an owner's personal information. The information storing apparatus includes: a personal information storing section storing thereon the personal information which is to be disclosed; an authentication processing section, which is a requester authentication section for performing authentication processing of the requester using requester characteristic information indicating a physical characteristic of the requester, the authentication processing section receiving a title of the requester from a belonging of the requester, and performing the authentication processing by a predetermined strictness of the authentication corresponding

to the title; an access level setting section for setting a level of the personal information to be disclosed to the requester to a level of the personal information predetermined corresponding to the title when the requester authentication section authenticates the requester as the accessible person; and a personal information output section for outputting a part of the personal information stored on the personal information storing section to the requester in accordance with the access level set-up by the access level setting section.

[0016] The summary of the invention does not necessarily describe all necessary features of the present invention. The present invention may also be a sub-combination of the features described above.

BRIEF DESCRIPTION OF THE DRAWINGS

[0017] Fig. 1 is a conceptual diagram of an owner's IC card.

[0018] Fig. 2 is a block diagram showing a configuration of the owner's IC card.

[0019] Fig. 3 is a table showing data stored on an accessible person information storing section.

[0020] Fig. 4 is a flow chart showing an operation of the owner's IC card.

[0021] Fig. 5 is a schematic diagram of a first alternative of the owner's IC card.

[0022] Fig. 6 is a block diagram of a second alternative of the owner's IC card.

[0023] Fig. 7 is a conceptual diagram of a third alternative of the owner's IC card.

[0024] Fig. 8 is a block diagram showing a configuration of the owner's IC card according to the third alternative.

[0025] Fig. 9 is a table showing data stored on the accessible person information storing section according to the third alternative.

[0026] Fig. 10 is a block diagram of the owner's IC card.

[0027] Fig. 11 is a table indicating data stored on the accessible person information storing section.

[0028] Fig. 12 is a table indicating data stored on the access level storing section.

[0029] Fig. 13 is a table indicating another example of data stored on the access level storing section.

[0030] Fig. 14 is a table indicating yet another example of the data stored on the access level storing section.

DETAILED DESCRIPTION OF THE INVENTION

[0031] The invention will now be described based on the preferred embodiments, which do not intend to limit the scope of the present invention, but exemplify the invention. All of the features and the combinations thereof described in the embodiment are not necessarily essential to the invention.

[0032] Fig. 1 is a conceptual diagram of an owner's IC card 100 according to an embodiment of the present invention. The owner's IC card 100 stores a plurality of kinds of owner's personal information. Then, a person who requests the owner's personal information (to be referred to as "requester" hereinafter) is authenticated using face information on the requester, and the access level for the personal information for the requester is set up. Here, the access level is a level of the personal information to be disclosed to a requester.

[0033] The owner's IC card 100 receives face information indicating characteristic of the face of the requester, e.g.,

a face image, from a requester's IC card 102 retained by the requester on radio, for example.

[0034] The owner's IC card 100 collates the received face information with template face information stored on the owner's IC card 100 to identify the requester. Then, the owner's IC card 100 sets up the access level for the personal information for the requestor and transmits a part of the personal information, which is allowed to be output in accordance with the set-up access level, to the requester's IC card 102 on radio, for example.

[0035] In this way, when setting the access level for the personal information, the owner's IC card 100 authenticates the requester based on the face information on the requester. For this reason, a person who does not have the authority for acquiring the personal information is not able to impersonate a requester having the acquisition authority.

[0036] Moreover, the owner's IC card 100 receives requester characteristic information from a predetermined IC card, i.e., the requester's IC card 102. Therefore, the owner's IC card 100 does not output the personal information to a person who does not retains the predetermined IC card.

[0037] In addition, the owner's IC card 100 is an example of the information storing apparatus storing thereon the owner's personal information in advance, and is retained by the owner. Moreover, the requester's IC card 102 is a portable apparatus retained by the requester, and includes the same or similar function as/to that of the owner's IC card 100. In another example, a portable remote terminal, such as PDA and a portable telephone, is used as the information storing apparatus instead of the owner's IC card 100 and/or the requester's IC card 102.

[0038] Moreover, the face information on the requester received from the requester's IC card 102 is an example of the

requester characteristic information indicating physical characteristic of the requester. Alternatively, the owner's IC card 100 receives data indicating characteristic of the face of the requester as the face information. Moreover, the template face information stored on the owner's IC card 100 is an example of the accessible person characteristic information indicating the physical characteristic of the accessible person. Alternatively, the owner's IC card 100 stores data indicating face image of the requestor or characteristic of the face of the requester as the template face information.

[0039] Fig. 2 is a block diagram showing a configuration of the owner's IC card 100. The owner's IC card 100 includes an accessible person information storing section 110, a requester authentication section 120, an access level setting section 130, a personal information storing section 140, and a personal information output section 150.

[0040] The accessible person information storing section 110 also functions as an access level storing section, and stores the access level information and the template face information in association with each of a plurality of accessible persons, to whom the personal information is to be disclosed. The access level information indicates the level of the personal information to be disclosed to the associated accessible person (to be referred to as "personal information level" hereinafter).

[0041] The requester authentication section 120 receives the face information on the requester from the requester's IC card 102. Then, the requester authentication section 120 performs authentication processing using the received face information and the template face information stored on the accessible person information storing section 110, and judges whether the requester is an accessible person.

[0042] When the requester is authenticated, the access level setting section 130 sets the access level for the requester based on the access level information stored on the accessible person information storing section 110. For example, the access level setting section 130 sets the access level to the personal information level indicated in the access level information. Accordingly, when the requester authentication section 120 authenticates the requester as an accessible person, the access level setting section 130 sets the access level to the personal information level corresponding to the accessible person.

[0043] The personal information storing section 140 stores the personal information on the owner of the owner's IC card 100. Alternatively, the personal information storing section 140 stores the personal information to be disclosed to a predetermined accessible person. The personal information output section 150 transmits a part of the personal information stored on the personal information storing section 140, which is allowed to be output in accordance with the access level set-up by the access level setting section 130, to the requester's IC card 102, and causes the requester's IC card 102 to store the part of the personal information.

[0044] By including such the compositions, the owner's IC card 100 authenticates the requester based on the face information on the requester and sets the access level for the personal information for the requestor, so that a part of the personal information, which is allowed to be output in accordance with the set-up access level, is transmitted to the requester's IC card 102.

[0045] Details of the accessible person information storing section 110 will be explained later using a table. Moreover, details of operation of the requester authentication

section 120, the access level setting section 130, and the personal information output section 150, will be explained later using a flow chart.

[0046] Fig. 3 is a table showing data stored on the accessible person information storing section 110. The accessible person information storing section 110 associates an ID number of accessible persons with the template face information on each of the accessible persons, and stores them. Accordingly, the accessible person information storing section 110 stores the template face information on a plurality of accessible persons in advance. Therefore, when the requester authentication section 120 acquires the ID number from the requester, the requester authentication section 120 selects the template face information used for the authentication of the requester from the accessible person information storing section 110 based on the ID number.

[0047] Moreover, the accessible person information storing section 110 stores the access level information in association with the ID number of each of the plurality of accessible persons. Each access level information indicates the personal information level to be disclosed for a corresponding accessible person. Therefore, when the ID number of the requester is acquired, the access level setting section 130 selects the personal information level to be disclosed to the requester from the accessible person information storing section 110 based on the ID number.

[0048] In addition, the access level information designates kinds of personal information, such as for example, medical information and family structure. In another example, the access level information designates an address of the personal information storing section 140 in which the personal information is stored.

[0049] Fig. 4 is a flow chart of an operation of the owner's IC card 100 when the owner's IC card 100 outputs the personal information to the requester's IC card 102. The requester authentication section 120 of the owner's IC card 100 receives the ID number of the requester and the face information of the requester from the requester's IC card 102 (S10). Then, the requester authentication section 120 selects and reads the template face information from the accessible person information storing section 110 based on the ID number of the requester (S20), and computes a correlation between the face information received from the requester's IC card 102 and the template face information (S30). If the computed correlation is greater than or equal to a predetermined reference value (S40: Yes), the requester authentication section 120 judges that the requester is the accessible person and authenticates the requester.

[0050] By this operation, the requester authentication section 120 authenticates the requester using the face information.

[0051] Then, based on the ID number of the authenticated requester, the access level setting section 130 reads the access level information corresponding to the accessible person identified by the ID number from the accessible person information storing section 110. Then, the access level setting section 130 sets the access level based on the read access level information (S50).

[0052] The personal information output section 150 outputs a part of the personal information, which is allowed to be output in accordance with the set-up access level, to the requester's IC card 102 (S60). Alternatively, the personal information output section 150 outputs the information indicating that the requester has been authenticated to the requester's IC card 102

before outputting the personal information. In this case, the requester's IC card 102 requests a part of the personal information to the output section 150, and the personal information output section 150 outputs only a part of the personal information, which is allowed to be output to the requester's IC card 102 in accordance with the set-up access level, among the part of the personal information requested by the requester's IC card 102.

[0053] Although the face information is employed as the requester characteristic information in the above-described embodiment, it is also possible to use fingerprint information indicating characteristic of a fingerprint of the requester, palm-print information indicating characteristic of a palm print of the requester, voiceprint information indicating characteristic of a voiceprint of the requester, etc. as the requester characteristic information.

[0054] Moreover, although the personal information output section 150 outputs the personal information to the requester's IC card 102, the personal information output section 150 may output the personal information to any equipment other than the requester's IC card 102.

[0055] Fig. 5 is a schematic diagram of the first alternative of the owner's IC card 100. In this alternative, the owner's IC card 100 is used with an information displaying apparatus 200 and an image capturing apparatus 300. For example, the information displaying apparatus 200 and the image capturing apparatus 300 are installed in a consultation room of a hospital etc.

[0056] The owner of the IC card inserts the owner's IC card 100 into the information displaying apparatus 200. The

requester inputs the requester's ID number into the information displaying apparatus 200.

[0057] The information displaying apparatus 200 causes the image capturing apparatus 300 to capture an image of the requester's face and to generate face information of the requester. Then, the information displaying apparatus 200 outputs the face information on the requester and the ID number of the requester to the requester authentication section 120 of the owner's IC card 100.

[0058] The requester authentication section 120 of the owner's IC card 100 selects the template face information from the accessible person information storing section 110 based on the received ID number of the requester. Then, authentication processing of the requester is performed based on the selected template face information and the face information received from the information displaying apparatus 200.

[0059] After the authentication processing is completed and the access level for the personal information has been set, the requester requests the personal information output section 150 of the owner's IC card 100 to output the personal information through the information displaying apparatus 200. The personal information output section 150 outputs the personal information to the information displaying apparatus 200 if the personal information is allowed to be output in accordance with the set-up access level. Then, the information displaying apparatus 200 displays the personal information.

[0060] According to the first alternative, the requester is authenticated by collating the face information generated at the time of the requisition of the personal information with the template face information. Therefore, a person who has not been registered on the accessible person information storing

section 110 cannot impersonate the registered person, and cannot acquire the personal information.

[0061] Fig. 6 is a block diagram of a second alternative of the owner's IC card 100. In the second alternative, the owner's IC card 100 further includes an image capturing section 115. When a requester requests the personal information, the image capturing section 115 captures an image of the requester, and generates face information of the requester.

[0062] Moreover, the requester authentication section 120 acquires the ID number of the requester from the requester's IC card 102 or the input section (not shown), and selects the template face information from the accessible person information storing section 110. Then, a correlation between the face information generated by the image capturing section 115 and the template face information is computed, and then the requester is authenticated. If the requester is authenticated, the access level setting section 130 sets the access level of the personal information for the requester.

[0063] According to the second alternative, the requester authentication section 120 authenticates the requester using the face information generated when the personal information is requested. Therefore, a person who is not registered on the accessible person information storing section 110 cannot impersonate a person who is registered, and cannot acquire the personal information. Moreover, since the image capturing section 115 of the owner's IC card 100 generates the face information on the requester, an external image capturing apparatus is not needed when authenticating the requester.

[0064] Moreover, since the image capturing section 115 of the owner's IC card 100 generates the face information on the requester, an external image capturing apparatus is not needed

when authenticating the requester. Therefore, the owner's IC card 100 sets the access level for the personal information and outputs the personal information at any place.

[0065] Fig. 7 is a conceptual diagram of a third alternative of the owner's IC card 100, and Fig. 8 is a block diagram showing a configuration of the owner's IC card 100 according to the third alternative. In the third alternative, the requester authentication section 120 of the owner's IC card 100 receives the face information and information indicating title of the requester from the requester's IC card 102 on radio, for example. Here, the title is information indicating a category to which a user belongs, e.g., a doctor, a pharmacist, a hygienist, a police officer, a lawyer, a teacher, etc. Moreover, the owner's IC card 100 further includes an image capturing section 115, which is an example of a physical information acquiring section. The image capturing section 115 captures an image of the face of the requester who retains the requester's IC card 102, and generates face information. In this case, the requester authentication section 120 collate the face information generated by the image capturing section 115 with the face information acquired from the requester's IC card 102, and then the requester is authenticated. If the requester authentication section 120 authenticates the requester, the access level setting section 130 judges that the information indicating the title acquired from the requester's IC card 102 is authentic, and sets the access level for the personal information in accordance with the information indicating the title.

[0066] According to the third alternative, the access level for the personal information for the requester is set in accordance with the title of the requester after the requester

has been authenticated. Therefore, a person who does not have the title cannot impersonate a person who has the title, and cannot acquire the personal information.

[0067] Alternatively, the owner's IC card 100 omits the image capturing section 115 and receives the face information of the requester generated by an external image capturing apparatus. In this case, the requester authentication section 120 collates the face information generated by the external image capturing apparatus with the face information of the requester received from the requester's IC card 102, and authenticates the requester.

[0068] Alternatively, the requester authentication section 120 authenticates the requester using fingerprint information indicating characteristic of a fingerprint or voiceprint information indicating characteristic of a voiceprint instead of the face information.

[0069] Fig. 9 is a table showing data stored on the accessible person information storing section 110 according to the present alternative. The accessible person information storing section 110 stores the information indicating the access level in association with the information indicating the title. By this, the access level setting section 130 sets the access level for the personal information for the requester in accordance with the title of the requester.

[0070] Figs. 10, 11, and 12 shows a fourth alternative of the owner's IC card 100. Fig. 10 is a block diagram of the owner's IC card 100. Except for the below-described explanation, since a component depicted in Fig. 10 which bears the same reference numeral as the component depicted in Fig. 6 has the similar function to the component depicted in Fig. 6, the explanation of such a component will be omitted.

[0071] In the present alternative, the owner's IC card 100 authenticates the requester using a plurality of physical characteristics received from the requester. In addition to the configuration of the owner's IC card 100 explained using Fig. 6, the owner's IC card 100 further includes an access level storing section 160 and a microphone 170. The access level storing section 160 stores the access level information. Moreover, the microphone 170 receives voice of the requester and generates voiceprint information on the requester.

[0072] Fig. 11 is a table indicating the data stored on the accessible person information storing section 110 in the present alternative. In the present alternative, the accessible person information storing section 110 stores the template face information and the template voiceprint information on the accessible person in association with the ID number of the accessible person. For examples, the template voiceprint information is information identifying the voiceprint of the corresponding accessible person. Moreover, the template face information and the template voiceprint information are examples of the accessible person characteristic information. Therefore, in the present alternative, the accessible person information storing section 110 stores a plurality of accessible person characteristic information on each accessible person in advance. Alternatively, the accessible person information storing section 110 stores other kinds of accessible person characteristic information, such as fingerprint information and palm print information instead of the template face information and the template voiceprint information.

[0073] Then, when the requester authentication section 120 performs authentication processing, the accessible person

information storing section 110 supplies the template face information and the template voiceprint information to the requester authentication section 120. Accordingly, the requester authentication section 120 receives a plurality of accessible person characteristic information. Moreover, the requester authentication section 120 receives the face information generated by the image capturing section 115 and the voiceprint information generated with the microphone 170 as a plurality of requester characteristic information corresponding to the accessible person characteristic information. Then, the requester authentication section 120 performs authentication processing of the requester using the plurality of accessible person characteristic information and the plurality of requester characteristic information.

[0074] In the authentication processing, the requester authentication section 120 computes the credibility of the authentication by comparing the plurality of accessible person characteristic information and the plurality of requester characteristic information. In this computation, the requester authentication section 120 computes the correlation between each of the plurality of accessible person characteristic information and each of the plurality of requester characteristic information. Then, the requester authentication section 120 computes the credibility of the authentication based on the computed correlation and standard deviation of sampling distribution of the physical characteristic. For example, the standard deviation is statistically computed in advance for the physical characteristic corresponding to each of the requester characteristic information.

[0075] Then, the requester authentication section 120 compares the computed credibility of the authentication with

a predetermined authentication criterion. Then, when the computed credibility of the authentication is greater than the authentication criterion, the requester authentication section 120 authenticates the requester as the accessible person.

[0076] Alternatively, the requester authentication section 120 computes the credibility of the authentication about each of the plurality of physical characteristics. Then, when the credibility corresponding to one of physical characteristics is greater than the authentication criterion, for example, the requester authentication section 120 authenticates the requester as the accessible person. Moreover, the requester authentication section 120 may perform authentication processing of the requester based on the plurality of credibility of the authentication corresponding to the plurality of physical characteristics.

[0077] In this way, in the present alternative, the requester authentication section 120 authenticates the requester using the plurality of physical characteristics. Therefore, even if one physical characteristic of the requester is so characterless that it is difficult to distinguish the requester from many persons who resemble the requester in the physical characteristic, the requester can be authenticated appropriately by using another physical characteristic.

[0078] Fig. 12 is the table indicating the data stored on the access level storing section 160 in the present alternative. The access level storing section 160 stores the access level information and the authentication criterion in association with the ID number of the accessible person. Accordingly, the access level storing section 160 stores the personal information level and the authentication criterion in association with each other.

[0079] Here, the access level information indicates the personal information level to be disclosed to the corresponding accessible person, for example. Moreover, the authentication criterion is strictness of the authentication when the personal information within the personal information level indicated in the corresponding access level information is to be disclosed, for example.

[0080] Moreover, in the present alternative, the access level storing section 160 stores a plurality of access level information corresponding to the plurality of accessible persons. Moreover, the access level storing section 160 stores the lower limit of the credibility of the authentication as an authentication criterion corresponding to each of the access level information.

[0081] Here, if a request for disclosure of the personal information is received from the requester, the requester authentication section 120 designates the access level information indicating the personal information level for the requested personal information, and reads the authentication criterion corresponding to the access level information from the access level storing section 160. Accordingly, the requester authentication section 120 receives the authentication criterion corresponding to the personal information level for the personal information requested from the requester from the access level storing section 160. Then, the requester authentication section 120 performs authentication processing of the requester using the received authentication criterion.

[0082] Accordingly, different authentication criteria can be used according to the levels of the personal information to be disclosed. In this case, the requester can be authenticated

with the required accuracy according to sensitivity and importance of the personal information, for example. It is preferable that the access level storing section 160 stores a higher authentication criterion for the sensitive information, such as medical information, for example. According to the present alternative, the personal information can be protected appropriately.

[0083] Fig. 13 is a table indicating another example of the data stored on the access level storing section 160 in the present alternative. In this example, the access level storing section 160 stores the access level information and the authentication criterion in association with the title of the requester. Moreover, the requester authentication section 120 receives the ID number of the requester and the title of the requester from the requester's IC card 102. Alternatively, the requester authentication section 120 receives the title of the requestor from a belonging of the requester.

[0084] Moreover, the requester authentication section 120 reads the authentication criterion corresponding to the received title from the access level storing section 160. Then, the requester authentication section 120 performs authentication processing of the requester using the received authentication criterion. In this case, the requester authentication section 120 performs the authentication processing based on the ID number of the requester and the information stored on the accessible person information storing section 110.

[0085] Then, when the requester authentication section 120 authenticates the requester as the accessible person, the access level setting section 130 reads the access level information corresponding to the title of the requester from the access level storing section 160. Then, the access level setting section

130 sets the access level to the personal information level indicated in the access level information. Accordingly, the access level setting section 130 sets the access level to the access level corresponding to the title of the requester. According to this example, appropriate level of the personal information can be disclosed according to the title of the requester.

[0086] Fig. 14 is a table indicating yet another example of the data stored on the access level storing section 160 in the present alternative. In this example, the access level storing section 160 stores a plurality of access level information in association with the ID number of each accessible person. The plurality of access level information may indicate different personal information levels from each other. Moreover, the access level storing section 160 stores the authentication criterion in association with each access level information. Each authentication criterion indicates the lower limit of the credibility of the authentication.

[0087] Moreover, in this example, the requester authentication section 120 supplies the computed credibility of the authentication to the access level setting section 130. The access level setting section 130 receives a plurality of authentication criteria corresponding to the ID number of the accessible person, which is identical to the ID number of the requester, from the access level storing section 160. Then, the access level setting section 130 compares the credibility computed by the requester authentication section 120 with each authentication criterion, and selects the authentication criterion less than the computed credibility.

[0088] Then, the access level setting section 130 reads the access level information corresponding to the selected

authentication criterion from the access level storing section 160. Accordingly, the access level setting section 130 selects a personal information level of which the corresponding authentication criterion is less than the credibility of the authentication computed by the requester authentication section 120. Then, the access level setting section 130 sets the access level to the sum of the selected personal information levels. In this way, when the requester authentication section 120 authenticates the requester by the authentication criterion or a criterion stricter than the authentication criterion, the access level setting section 130 determines the personal information level corresponding to the authentication criterion as at least a part of the access level.

[0089] Hereafter, operation of the owner's IC card 100 will be exemplary explained. In this example, the access level storing section 160 stores a plurality of levels C, D and E in association with the ID number 002 of the accessible person. Moreover, the access level storing section 160 stores lower limits 90%, 20% and 40% as authentication criteria corresponding to the plurality of levels C, D and E, respectively.

[0090] Therefore for example, when the ID number of the requester is 002, the access level setting section 130 sets the access level to some or all of the levels indicated in the access level information corresponding to the accessible person whose ID number is 002. For example, when the credibility computed by the requester authentication section 120 is 50%, the access level setting section 130 selects the levels D and E corresponding to 20% and 40%, which are authentication criteria less than 50%. Then, the access level setting section 130 sets the access level to the sum of the level D and the level E. Moreover, when the credibility computed by the requester authentication section

120 is 30%, the access level setting section 130 sets the access level to the level D corresponding to 20%, which is the authentication criterion less than 30%.

[0091] Here, there is the personal information having high sensitivity and importance which is to be disclosed after performing strict authentication, such as medical information. On the other hand, some personal information has low sensitivity and importance and can be disclosed with simple authentication. Moreover, in the authentication using a physical characteristic, if one's face resembles others', for example, it may be difficult to authenticate with one hundred percent credibility.

[0092] Therefore, when the authentication for disclosing the personal information is performed by the uniform authentication criterion regardless of the kind of the information, authentication may become excessively simple or strict. However, according to this example, the appropriate strictness of the authentication can be set according to the kind of the information. Accordingly, the access level can be changed according to the credibility of the authentication. According to this example, personal information can be protected appropriately.

[0093] As described above, according to the present invention, there is provided the information storing apparatus for setting the access level for the information for the requester of the information, and for preventing a person without authority to impersonate a person with authority to acquire the information.

[0094] Although the present invention has been described by way of an exemplary embodiment, it should be understood that those skilled in the art might make many changes and substitutions without departing from the spirit and the scope of the present

invention. It is obvious from the definition of the appended claims that embodiments with such modifications also belong to the scope of the present invention.